# Point. Click. Cloud.

## The case for cloud governance

By **John Heaton**
Partner, Advisory
KPMG in Canada

The age of online data comes with great potential. Yet as concerns over data protection and client privacy mount, organizations are growing wise to the reality that selecting and leveraging cloud collaboration solutions is not as simple as point, click, cloud.

No doubt, the need for cloud governance is rising. And with more and more solutions coming online, organizations are being challenged to embrace these innovations while mitigating the significant risks therein. To do so, they must design policies and controls around their own individual structures, demands, workforce, and unique risk environments.

There is no cookie-cutter approach to cloud governance. Even so, it can help to see how others are facing this lofty challenge.

### A host of options

Cloud-based solutions can be broken down into three separate tiers. Each requires unique considerations when it comes to their intended use, users, and potential for risk.

They include:

- **Tier 1: Enterprise solutions** (e.g., SalesForce, MS Azure, Office 365): The size and reputation of the solution provider are important considerations when procuring Tier 1 solutions, especially in regards to data security.
- **Tier 2: Consumer solutions** (e.g., GoogleDrive, DropBox, and Prezi): These solutions are readily available and easily accessible online, making them a convenient data-sharing option, but a liability if used irresponsibly or without proper controls. To that end, a number of companies have outright prohibited the use of Tier 2 cloud-based services by their employees.
- **Tier 3: Start-Up solutions:** These are cloud services designed for specific industry vertical or business functions and selected on a case-by-case basis (e.g. Accounting).

Defining controls for each will again come down to experience. And indeed, one prominent pension fund company noted, "We have not formally defined the Tiers, however, our experience gained as cloud services are being adopted is guiding our thought process on adopting a Tiering classification approach."

### Procurement

Options for storing and sharing data online have grown exponentially in recent years. From Google to OneDrive, DropBox and beyond, the virtual shelves are crowded with "next best solution". As such, it can be difficult to find a service that fits.

There are key differences between cloud-based services in regards to their intended use, accessibility, and data ownership. For example, some solutions may provide data encryption and security as part of their fee-based service, while others might place the onus of data protection on the user themselves. Then, there are solutions that offer their resources for free in exchange for the right to use any uploaded material for marketing purposes without permission from the original owner.

Navigating these options is no small challenge; and when it comes to procurement, organizational strategies differ. For example, some clients have entrusted the entire procurement process to their IT departments, while others have split the task among various departments with oversight from the IT professionals.

As one leading employee-owned investment manager explained, the size of an organization can be a factor: "As a small organization, it is easier but both IT, operations and legal have to be involved in selecting a proper solution always keeping in mind the cyber security risks and always aiming to protect the precious data."

Whether the decision makes it to the boardroom or not, the consensus among those I've spoken with is that IT needs to be part of the cloud-based solution procurement. To what extent the department has in making the final decision – or even owning the process outright – can vary based on how much authority business leaders are comfortable passing down.

### Setting the policy

Making the most of cloud-based services means establishing policies and procedures that ensure they are used safely and responsibly. This means creating cloud governance policies that dictate who can use them, how and when they can be used, and what type of data is permitted.

There are standards in place to help in crafting a cloud governance policy. Enterprise Architecture, for example, is used by many organizations to ensure an industry-accepted approach to enterprise analysis, design, planning, and implementation.

Offering its own approach for example, one large-scale pension fund organization shared: "The organization has architectural governance standards in place which set appropriate use guidelines for cloud services. These Standards are currently sponsored by Enterprise Architecture but maintained and applied by a cross functional architectural governance body...We also have a formal information security due diligence review process for cloud services that store and/or process our information. If personal information is involved, there is an additional review process regarding privacy-related controls."

The question of who owns an organization's cloud governance policies can also vary. Once again, some organizations have given IT the responsibility to determine policies and procedures around the use of such solutions, while others have handed the task to department leaders, while leaving maintenance, policy updating, and assurance activities to IT staff.

Trusting an outside party is also an option. According to a top investment firm: "We have retained the services of an external, third-party provider to establish the cloud infrastructure and of another cybersecurity firm to oversee the structure's security."

## Ensuring controls

Common controls for cloud-based services include URL blocking, ongoing technical and manual surveillance, monthly scanning for unknown cloud services, and blocking/alerting for highly sensitive documents.

Setting those controls is, however, the first step. The next, is gaining assurance over the cloud provider's own processes and controls. To that end, it is common practice for procurement to perform upfront due diligence. This can include evaluating service-level agreement (SLA) commitments, Service Organization Controls (SOC) 2 reports, or ISO certifications as part of the selection and procurement process. Similar risk-based approaches are also applied during the engagement and at the termination of a service.

Recalling its own approach, the same investment firm recalled: "Before selecting the firms, we scoped the industry in order to identify the service providers that best suited our needs as a firm...then, we entered into agreements with both its infrastructure provider as well as its cybersecurity consultants which outline the roles, responsibilities, and liabilities of each service provider."

## A culture of data security

There's no discounting the human factor in cloud governance. Policies and procedures are nothing without a staff that understands the risks of sharing their data online and is adhering to established rules.

Herein, organizations would do well to invest in training on cloud governance standards and the organization's policy on data classification.

As a large-scale pension fund organization shared: "Our organization's Information Security Program includes awareness training and Corporate Information Security Policy and the Code of Conduct sets explicit expectations for user behaviour."

## High expectations

Cloud-based solutions aren't uncharted territory. In recent years, however, the surge of cyber events and data breaches has re-affirmed the need for stronger cloud governance. In so doing, organizations can manage how much risk they are prepared to assume, and how they balance the need to control these cloud solutions while keeping pace with the new and innovative tools that are being created.

## Risk management

Any disruptive technology requires a strong risk management approach. Consider the following when integrating a cloud-based service:

**A united front:** It takes a buy-in from all stakeholders to keep strategic risks in focus. That includes the board, management, and both front and back-end employees.

**Diligent monitoring:** Keep a constant eye on market conditions and changes, new regulations, and shifts in both your external clients and internal operations.

**Agile:** Encourage a culture of awareness around strategic risks and be ready to respond to changes and emergencies.

**Expert collaboration:** Seeking expert, third-party assistance can go a long way towards identifying potential risks, assessing your current state, and designing a roadmap for cloud-based service integration.

Source: Strategic risks: Learning from blockchain and other potential disruptors, KPMG 2018

**Contact:**
**John Heaton**
Partner, Advisory
KPMG in Canada
johnheaton@kpmg.ca

kpmg.ca/rethinkrisk
#rethinkrisk